Serial No.: 10/776,407

REMARKS

Claims 1, 5-7, and 11-12 are pending in the application. Claims 8 has been amended to correct a typographical error. Favorable reconsideration of the application is respectfully requested.

I. REJECTION OF CLAIMS UNDER 35 USC § 103

Claims 1, 5-8, and 11-12 stand rejected under 35 USC 103 as being unpatentable over US Patent 6,327,578 to Linehan in view of US Patent 6,061,449 to Candelore et al.

General Discuss of Linehan

Linehan teaches a system for credit card processing where a merchant obtains an authorization token approving a credit card transaction from a credit card issuing system through the consumer's system (called a wallet) as shown in Figure 2a or directly from the issuer system as shown in Figure 4 (C8, L16-L19). The merchant passes the authorization token to the merchant's bank over the Internet and payment against the authorization is requested by the merchant's bank over a private network. (See generally Figure 2a)

To assure that the authorization from the credit card issuer is valid, the following process shown in Figure 3 used:

1. The merchant sends a wallet initiation message to the consumer. The wallet initiation message includes the payment amount and is digitally signed by the Merchant (Figure 3, Step 304).

2. The Consumer authenticates himself or herself to the wallet software using a User ID/Password combination (Figure 3, step 306).

3. The wallet software sends the initiation message to a gateway system of the credit card issuer (Figure 3, step 306).

4. The Issuer verifies the merchant's digital signature (Figure 3, step 308)

5. If authorized, the Issuer sends a signed authorization token along with the Issuer's certificate. The signed authorization token comprises the initiation message and a reference to the consumer's credit card (Figure 3, step 310).

6. The consumer passes the authorization token to the merchant.

In a variation, the authorization token may be passed directly to the merchant (Figure 4 and C8, L16-L19).

In another variation a smart card is used to authenticate the consumer. Prior to generating the authorization token, the Issuer can verify that the consumer's smart card is present by passing a challenge message to the consumer computer which passes the challenge to the smart card reader which passes the challenge to the smart card. The smart card signs the challenge with its digital signature and returns the signed challenge response. The issuer verifies the smart card's signature to verify the consumer's identity. (Figure 2C and C7, L21-L38).

It must be appreciated that in all of the systems disclosed by Lineham, the authorization token is generated by passing the transaction (or an indication of the transaction) to the issuer gateway and then the authorization token is generated by the issuer gateway. The processed used by the issuer for generating the authorization token is shown in Figure 8. This is distinct from applicant's invention wherein the authorization message is generated by the remote system using a unique multi-step process wherein it can be generated without a need to transfer the electronic fund transfer disbursement file to the remote system.

Independent Claim 1

The examiner cites Linehan (C7, L55 to C, L15) as teaching authentication in a remote system via the Internet. The applicant acknowledges, without traverse, that Linehan teaches a system for authorizing a payment at a remote system.

However, the applicant respectfully asserts that the system taught by Linehan does not anticipate, or render obvious, the applicant's method for operating a server

which, as part of a method for generating an electronic fund transfer submission, obtains an authorization message from a remote system in a unique manner. More specifically:

1. The examiner asserts that Linehan teaches *"a merchant generating an authorization request which includes payment amount, order description, timestamp, a random nonce, and possible additional data depending upon requirements (column 9, lines 35-40). The authorization request can also include a hash of an order description instead of the actual order description (column 16, lines 18-25). The authorization request or has is transferred to a remote system (column 14, lines 28-31).*

The applicant does not traverse the examiner's position that such steps are equivalent to the applicant's server: i) generating a digest of the electronic fund transfer disbursement file; and ii) transferring the digest to the remote system.

2. The examiner asserts that Linehan teaches *"Once the authorization request/hash is sent to the consumer computer, the request gets sent to consumer's/issuing bank and verifies the merchant's signature to prove the consumer is dealing with the actual merchant and validates the merchant's certificate and the acquirer's certificate (column 6, lines 8-12, column 15, lines 25-32)".*

The applicant respectfully asserts that such step does not anticipate, or render obvious, applicants server "transferring authorization control code to the remote system, the authorization control code being executed by the remote system to: i) generate the authorization message on the remote system; and ii) return the authorization message to the server" because:

a) Linehan does not teach how the request "gets sent to" the consumer's/issuing bank and Linehan implies that the executable code for doing so (e.g. the wallet) is on the consumer's computer. More specifically,

Linehan provides no teaching of transferring any control code to be executed by the remote system. Linehan only teaches transferring the authorization request (which the examiner asserts is comparable to applicants step of transferring the digest to the remote system) - and there is no teaching that the authorization request includes any control code to be executed by the remote system in the authorization request;

b) Even if Linehan taught some transfer of code to be executed by the remote system, there is no teaching that such code, when executed, provides for the remote system to generate an authorization message using applicant's defined steps and to return such authorization message to the server.

3. The examiner asserts that Linehan teaches *"Sending over the Internet network an authorization token, an issuer's digital certificate, and a reference to the consumer's credit or debit card number. The authorization token includes the payment amount, order description, time stamp, a random nonce, the merchant identifier from the merchant's digital certificate, and the acquiring bank identifier from the acquiring bank's digital certificate, plus a reference to the consumer's credit or debit card number (Column 25, lines 36-44).*

The applicant acknowledges, without traverse, the examiner's position that such steps are equivalent to the applicant's steps of: i) generating additional message attributes and generating authenticated attributes comprising the additional message attributes and the digest.

However, the applicant's invention remains distinguishable over Linehan because, in the applicant's invention as set forth in claim 1, these steps are part of generating an authorization response message by execution of control code transferred to the remote system the Server. As discussed above, Linehan does not teach, or suggest that the merchant 204 transfers any code executable by the consumer system 202. More specifically, Linehan does not teach or suggest that the

merchant 204 transfers any code executable the remote system for performing such processes.

4. The examiner asserts that Linehan teaches *"The merchant presenting the authorization code to a payment processor in order to complete the transaction (column 6, lines 48-55, column 16, lines 6-8).*

The examiner further asserts that Linehan teaches *"The authorization includes a combination of payment amount, order description, timestamp, a random nonce, and possible additional data depending upon requirements (column 9, lines 35-40). The authorization request can also include a hash of an order description instead of the actual order description (column 16, lines 18-25).*

The applicant acknowledges, without traverse, the examiner's position that such step is comparable to applicant's server "combining the electronic fund transfer disbursement file with the authorization message to create the electronic fund transfer submission; and transferring the electronic fund transfer submission to the payment processor.

5. The examiner asserts that Linehan teaches *"The system can also generate dummy data (column 11, lines 3-9), in combination with the payment amount, order description, timestamp, a random nonce, the merchant identifier from the merchant's digital certificate, and the acquiring bank identifier from the acquiring bank's digital certificate, plus a reference to the consumer's credit or debit card number (column 25, lines 36-44).*

In the applicant's invention, the "dummy data string" is used for generating a dummy authorization message with the predetermined data structure of an authorization message. The authorization message is then generated by making the following replacements within the dummy authorization message: i) replacing the digest of the dummy data string with the digest of the electronic fund transfer

disbursement file as provided by the server; and ii) replacing the digital signature of the digest of the dummy data string with the digital signature of the digest of the electronic fund transfer disbursement file.

First, the applicant respectfully asserts that the examiner's interpretation of "replacing dummy data with real data" as a function in which a message is hashed (examiner's point 3 in the office action), is an incorrect interpretation.

In view of the specification P16, L25 to P17, L2, it is clear that "replacing" is not a "hash function" but a "substitution function". The specification specifically states "to build the authentication data structure 123 for the authentication response 112, the authorization control code 107 replaces the dummy digest 129 in the dummy data structure 127 with the digest 104 from the authorization request 102". This is language of a "substitution" – not a "hash".

Second, column 11, lines 3-9 of Linehan indicate that a dummy card number referenced by Linehan is a card number used for routing the payment to an appropriate issuer. Further, Linehan indicates that the purpose of the random nonce – which could be interpreted as "dummy data" – is to "recognize duplicate tokens" (C16, L4-5).

The applicant respectfully asserts that neither Linehan's dummy card number nor Linehan's random nonce anticipates, or renders obvious, the applicant's Server providing control code executable on the remote system to:

i) generate a dummy data string;

ii) generate a dummy authorization message with the predetermined data structure by passing the dummy data string to the file authentication component of the remote system as part of an authorization response request. The dummy authorization message including a digest of the dummy data string; a digital signature of the digest of the dummy data string, and a digital certificate corresponding to the digital signature; and

iii) generate the authorization message from the dummy authorization message

by making the following replacements within the dummy authorization message: i) replacing the digest of the dummy data string with the digest of the electronic fund transfer disbursement file as provided by the server; and ii) replacing the digital signature of the digest of the dummy data string with the digital signature of the digest of the electronic fund transfer disbursement file.

The examiner further asserts that Candelore et al. *"...teaches an invention in which encrypted, authenticated information and dummy data are securely communicated between an external memory and a cryptographic ASIC in cipher block chains (column 17, lines 61-64). Modern cryptographic applications often employ public key cryptography, which generally require large keys than secret key cryptography. The scrambling sender or descrambling receiver may perform some type of cryptographic application which may interface on an open network such as the Internet, which may require the storing of a number of various public keys, e.g. from a Root Authority, or Certificate Authority (column 8, lines 65, 67, column 9, lines 1-6). If a pirate changes any data in preceding blocks in the chain from trailing, the computed hash data that is compared with the authentication information will be incorrect, and the resulting verification value will not match (column 12, lines 7-10). According to Candelore et al., the dummy is authenticated just like any other data in the process (column 23, lines 38-58). Therefore, in view of Candelore et al.'s teaching, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to combine Linehan's invention in view of Candelore et al. for authenticating dummy data just like any other data in the process. It would have been obvious so one skilled in the art to authenticate dummy data because it would confuse the pirate attempting to analyze the authenticated data (column 23, lines 53-55)".*

The teachings of Candelore et al. relate to storing program information on a disk (or other storage) in an encrypted manner to avoid pirating.

Not only does Candelore et al. use chain block encryption, but the blocks are

read from the storage device in a random sequence and dummy data blocks may be communicated between the storage and the secure circuit to further obfuscate the program information. Further, dummy data may be intermixed with encrypted data blocks to further obscure the data – or, in the examiners words, "to confuse the pirate attempting to analyze the authenticated data"

First, the applicants respectfully assert that the examiner's combination of Candelore et al. with Linehan et al. is inappropriate because neither reference suggest such a combination. More specifically, the generation and use of dummy data as taught by Candelore et al. (a system for storing data and protecting the data from piracy) if of no practical use in an authorization system such as Linehan. While Linehan uses a random nonce in a particular data field to distinguish duplicate authorization tokens and a dummy account number in a particular data field for routing, there is no practical need for incorporating dummy data with real data in an authorization token for purposes of obscuring.

Further, even if it were proper to combine the two references, neither Linehan nor Candelore et al. teach or suggest the a system wherein a Server provides control code executable the remote system to:

i) generate a dummy data string;

ii) generate a dummy authorization message with the predetermined data structure by passing the dummy data string to the file authentication component of the remote system as part of an authorization response request. The dummy authorization message includes a digest of the dummy data string; a digital signature of the digest of the dummy data string, and a digital certificate corresponding to the digital signature; and

iii) generate the authorization message from the dummy authorization message by making the following replacements within the dummy authorization message: i) replacing the digest of the dummy data string with the digest of the electronic fund transfer disbursement file as provided by the server; and ii) replacing the digital

signature of the digest of the dummy data string with the digital signature of the digest of the electronic fund transfer disbursement file.

Independent Claim 7

As previously discussed with respect to claim 1, the applicant does not traverse the examiners assertion that Linehan teaches a system for authorizing a payment at a remote system.

However, the applicant respectfully asserts that the system taught by Linehan does not anticipate, or render obvious, the applicants method for operating a server which, as part of a method for generating an electronic fund transfer submission, obtains an authorization message from a remote system.

As discussed with respect to claim 1, the examiner asserts that Linehan teaches *"The system can also generate dummy data (column 11, lines 3-9), in combination with the payment amount, order description, timestamp, a random nonce, the merchant identifier from the merchant's digital certificate, and the acquiring bank identifier from the acquiring bank's digital certificate, plus a reference to the consumer's credit or debit card number (column 25, lines 36-44)."*

In the applicant's invention, the "dummy data string" is used for generating a dummy authorization message with the predetermined data structure of an authorization message.

The dummy authorization message includes: i) a digest of the dummy data string; ii) a digital signature of the digest of the dummy data string; and a digital certificate corresponding to the digital signature.

The authorization message is then generated by making the following replacements within the dummy authorization message: i) replacing the digest of the dummy data string with the digest of the electronic fund transfer disbursement file as provided by the server; and ii) replacing the digital signature e of the digest of the dummy data string with the digital signature of the digest of the electronic fund transfer

disbursement file.

First, the applicant respectfully asserts that the examiner's interpretation of "replacing dummy data with real data" as a function in which a message is hashed (examiner's point 3 in the office action), is an incorrect interpretation.

Again, in view of the specification P16, L25 to P17, L2, it is clear that "replacing" is not a "hash function" but a "substitution function". The specification specifically states "to build the authentication data structure 123 for the authentication response 112, the authorization control code 107 replaces the dummy digest 129 in the dummy data structure 127 with the digest 104 from the authorization request 102". This is language of a "substitution" – not a "hash".

Second, Linehan, at column 11, lines 3-9 indicates that a dummy card number is a card number used for routing the payment to an appropriate issuer. Further, Linehan indicates that the purpose of the random nonce – which could be interpreted as "dummy data" – is to "recognize duplicate tokens" (C16, L4-5).

The applicant respectfully asserts that neither Linehan's dummy card number nor Linehan's random nonce anticipates, nor renders obvious, the applicants method which:

i) generates a dummy data string;

ii) generates a dummy authorization message with the predetermined data structure by passing the dummy data string to the file authentication component of the remote system as part of an authorization response request. The dummy authorization message including a digest of the dummy data string; a digital signature of the digest of the dummy data string, and a digital certificate corresponding to the digital signature; and

iii) generates the authorization message from the dummy authorization message by making the following replacements within the dummy authorization message: i) replacing the digest of the dummy data string with the digest of the electronic fund transfer disbursement file as provided by the server; and ii) replacing

the digital signature of the digest of the dummy data string with the digital signature of the digest of the electronic fund transfer disbursement file.

Again, the applicant respectfully asserts that the examiner's combination of Candelore et al. with Linehan et al. is inappropriate because neither reference suggest a combination. More specifically, the generation and use of dummy data as taught by Candelore et al. (a system for storing data and protecting the data from piracy) if of no practical use in an authorization system such as Linehan. While Linehan uses a random nonce in a particular data field to distinguish duplicate authorization tokens and a dummy account number in a particular data field for routing, there is no practical need for incorporating dummy data with real data in an authorization token for purposes of obscuring.

Again, the applicant respectfully asserts that even if the two references are combined, neither Linehan nor Candelore et al. teach or suggest the a method which comprises:

i) generating a dummy data string;

ii) generating a dummy authorization message with the predetermined data structure by passing the dummy data string to the file authentication component of the remote system as part of an authorization response request. The dummy authorization message includes a digest of the dummy data string; a digital signature of the digest of the dummy data string, and a digital certificate corresponding to the digital signature; and

iii) generating the authorization message from the dummy authorization message by making the following replacements within the dummy authorization message: i) replacing the digest of the dummy data string with the digest of the electronic fund transfer disbursement file as provided by the server; and ii) replacing the digital signature of the digest of the dummy data string with the digital signature of the digest of the electronic fund transfer disbursement file.

Claims 5, 6, 8, 11, and 12.

Each of claims 5, 6, 8, 11 and 12 depend from one of independent claims 1 or 7 and therefore can be distinguished over Linehan, Candelore et al. and the other art of record for the same reasons. Further, the additional elements and or steps recited in such claims further distinguish such claims over Linehan, Candelore et al. and the other art of record.

Claim 8

With specific reference to claim 8, neither Linehan, Candelore et al. nor the other art of record teaches or suggests the following steps in addition to the steps discussed above with respect to claim 7.

generating the digital signature of the authenticated attributes by passing the authenticated attributes to a digital signature hardware key as part of a digital signature request message and receiving, in response, the digital signature of the authenticated attributes; and

generating the dummy authorization response message comprises passing the dummy data string to the digital signature hardware key as part of an authorization response request message and receiving, in response, the dummy authorization response message in the predetermined data structure.

II. CONCLUSION

Accordingly, claims 1, 5-8, and 11-12 are believed to be allowable and the application is believed to be in condition for allowance. A prompt action to such end is earnestly solicited.

Should the Examiner feel that a telephone interview would be helpful to facilitate favorable prosecution of the above-identified application, the Examiner is invited to contact the undersigned at the telephone number provided below.

Serial No.: 10/776,407

Should a petition for an extension of time be necessary for the timely reply to the outstanding Office Action (or if such a petition has been made and an additional extension is necessary), petition is hereby made and the Commissioner is authorized to charge any fees (including additional claim fees) to Deposit Account No. 501825.

Respectfully submitted,

Timothy P. O'Hagan
Reg. No. 39,319

DATE: 3-17-06

Timothy P. O'Hagan
8710 Kilkenny Ct
Fort Myers, FL 33912
(239) 561-2300